REMARKS:

Claims 105-107, 109-118 and 127-167 were pending in the application. Claims 106, 116, 157-158, 160-161 and 167 have been canceled. Claims 105, 107, 115, 118, 127-128, 135-139, 142-143, 145, 147-148, 152, 155, 159 and 164 have been amended. Therefore, claims 105, 107, 109-115, 117-118 and 127-156, 159, 162-166 are now pending in this application.

Claim 105

The Examiner rejected the previous version of claim 105 under § 103 based on a proposed combination of Muttik (U.S. Patent No. 6,775,780) and Chess (U.S. Patent No. 6,772,346). While Applicant believes the previously pending claims patentably distinguish over this proposed combination, Applicant has nonetheless amended the claims to advance prosecution.

Claim 105 has been amended to include a feature previously found in claim 115: an "active program … running on the computer system in a manner that permits the program to infect the computer system." Neither Muttik nor Chess teaches this feature. Applicant respectfully notes that the present Office Action does not appear to address this feature of claim 115.

As Applicant has noted in the context of the prosecution of the parent application 10/231,557, Muttik (the primary reference cited by the Examiner in the present Office Action) teaches an emulator buffer 201 and emulator code 203 that "are designed so that code 108 that is executing within emulator buffer 201 cannot damage or compromise computer system 106." Muttik at col. 3, lines 63-65. Muttik can thus be said to represent a "sandbox"-type approach to the detection of malicious code.

In contrast, as noted above, the "code under investigation" in claim 105 is an "active program … running on the computer system in a manner that permits the program to infect the computer system." The analysis of this type of "active program" is not taught or suggested by Muttik, given the excerpt cited above. Furthermore, it would not be obvious to modify Muttik to permit its code 108 to run "in a manner that permits [code 108] to infect the computer system."

It cannot be said that there is a suggestion to modify a reference when the proposed modification would render the reference inoperable for its intended purpose. *See* MPEP § 2143.01, Section V, entitled "THE PROPOSED MODIFICATION CANNOT RENDER THE PRIOR ART UNSATISFACTORY FOR ITS INTENDED PURPOSE" ("If proposed modification would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification.").[1] **Here, any proposed suggestion to modify Muttik to teach the above-quoted limitation of claim 105 would render Muttik inoperable for its stated purpose of preventing "damage" to computer system 106.** As such, Muttik is believed to be (fatally) deficient as a primary reference in the context of a § 103 rejection. For at least this reason, Applicant submits that claim 105 is patentably distinct over the proposed combination of Muttik and Chess.[2]

More broadly, however, Applicant wishes to note that claim 105 represents a fundamentally different approach to malicious code detection than the approaches embodied by Muttik, Chess, and Kouznetsov. First of all, none of these references teaches or suggest "an active program ... running on the computer system in a manner that permits the program to infect the computer system" as the "code under investigation." Muttik, as noted above, uses the very different approach in which the code under investigation is "sandboxed" to prevent damage to the computer system. Chess does not appear to be concerned with the problem of discerning whether an "active program" as recited in claim 105 is malicious code; instead, it is merely concerned with "efficiently managing the transmission of units of digital data from node to node" "[i]n a network-connected distributed system" (e.g., to determine whether a particular file is a virus). *See* Chess (Abstract, Background). While Kouznetsov is directed to "behavorial analysis of runtime state," Kouznetsov (Title), as stated in the previous response, the programs

[1] *In re Gordon*, 733 F.2d 900, (Fed. Cir. 1984) (claimed device was a blood filter assembly for use during medical procedures wherein both the inlet and outlet for the blood were located at the bottom end of the filter assembly, and wherein a gas vent was present at the top of the filter assembly. The prior art reference taught a liquid strainer for removing dirt and water from gasoline and other light oils wherein the inlet and outlet were at the top of the device, and wherein a pet-cock (stopcock) was located at the bottom of the device for periodically removing the collected dirt and water. The reference further taught that the separation is assisted by gravity. The Board concluded the claims were prima facie obvious, reasoning that it would have been obvious to turn the reference device upside down. The court reversed, finding that if the prior art device was turned upside down it would be inoperable for its intended purpose because the gasoline to be filtered would be trapped at the top, the water and heavier oils sought to be separated would flow out of the outlet instead of the purified gasoline, and the screen would become clogged.).

being analyzed in Kouznetsov are not "running on the computer system in a manner that permits the program to infect the computer system." *See* Applicant's Response to Office Action of December 12, 2007 at 13-14 (discussing claim 106 and Kouznetsov's "logical shim" that intercepts system calls). Accordingly, none of the three references cited by the Examiner is directed to analysis of an "active program" as recited in claim 105.

Still further, however, note that claim 105 recites "successively executing each of a first and a second plurality of detection routines" to obtain first and second scores, respectively. Then, "upon completing the executing of the first and second plurality of detection routines," the first and/or second scores are used to "categorize the code under investigation." This sequence of events is neither taught or suggested by the cited art. Consider Muttik and Kouznetsov (Chess is wholly inapplicable), which, while different from one another, can both be considered to be "event"-based approaches to malicious code detection, as they "wait" for system calls to be made by the code under investigation. In contrast, the method of claim 105 selects an active program, successively executes each of the recited first and second plurality of detections routines, and, upon completion, categorizes the code under investigation using results of the executed detection routines. Stated another way, Muttik and Kouznetsov do not teach or suggest "successively executing" detection routines as recited in claim 105 and then categorizing the code under investigation upon completion of the executing. Claim 105 embodies a "scan and convict"-type approach that stands in contrast to the approaches in any reference cited by the Examiner. The approach of claim 105 may be used, for example, to more quickly categorize active programs, particularly when the approach is applied to multiple active programs (e.g., as in claim 107).

For at least this further reason, claim 105 is believed to be patentably distinct over the cited references. Claim 105's dependent claims are believed to be patentably distinct for at least the reasons provided for claim 105. Independent claims 115, 127, 128, 152, and 159 are believed to be patentably distinct (along with their respective dependent claims) for at least reasons similar to those provided above in support of claim 105.

Applicant therefore respectfully requests removal of the § 103 rejections.

---

[2] Chess appears to be cited only for the proposition of using a database of known malicious/non-malicious files as a point of comparison. Applicant submits that Chess has nothing to do with analysis of an "active program" as recited in claim 105.

CONCLUSION:

Applicants submit the application is in condition for allowance, and an early notice to that effect is requested.

If any extension of time (under 37 C.F.R. § 1.136) is necessary to prevent the above-referenced application from becoming abandoned, Applicant hereby petitions for such extension.

The Commissioner is authorized to charge any fees that may be required, or credit any overpayment, to Meyertons, Hood, Kivlin, Kowert & Goetzel, P.C. Deposit Account No. 501505/6002-00602/DMM.

Respectfully submitted,

Date: June 6, 2008

By: /Dean M. Munyon/
Dean M. Munyon
Reg. No. 42,914

Meyertons, Hood, Kivlin, Kowert & Goetzel, P.C.
P. O. Box 398
Austin, Texas 78767
(512) 853-8847